Square-class collisions and complete fourth moments for two split quartics

Brice Pouly

Research and writing with AI assistance

hexagon:2611.01197v1

Abstract

We count ordered quadruples of distinct integers $2 \le n_i \le X$ for which the product of the four values of $F(n) = n(n+1)(n+2)(n+3)$ is a square. The count is $O_\varepsilon(X^{5/3+\varepsilon})$, with no restriction on the square parts. The identity $F(3n-3) = 9G(n)$ gives the same bound for $G(n) = n(n-1)(3n-1)(3n-2)$. Two uniform estimates drive the proof. A prescribed nonidentity square class contains $O_\varepsilon(X^{2/3+\varepsilon})$ ordered pair products. The number of arguments whose squarefree kernel is at most T and divisible by a prescribed squarefree q is $O_\varepsilon(X^\varepsilon \min\{1 + X/q, \sqrt{T/q}\})$. The count gives a complete fourth-moment asymptotic for independent fair signs on the primes extended completely multiplicatively. With common signs the two sums have normalized mixed fourth moment tending to $11/9$, reflecting their overlap. A uniformly sampled unordered pair is determined by its product class with error $O_\varepsilon(X^{-1/3+\varepsilon})$.

1 When four values make a square

The product of four consecutive integers is one below a square.

$$F(n) = n(n+1)(n+2)(n+3) = (n^2+3n+1)^2 - 1.$$

No positive value is a square, yet products of different values can be squares. For an integer $m > 0$, write $m = \mathrm{sf}(m)a^2$ with $\mathrm{sf}(m)$ squarefree and a a positive integer. Thus $\mathrm{sf}(m)$ records the primes of odd valuation. At the four arguments $2, 3, 5, 7$, the kernels of F are $30, 10, 105, 35$. The pairs $\{2, 7\}$ and $\{3, 5\}$ both have product kernel 42. Here the two pair products are even equal, although the four kernels are distinct. The four values multiply to 604800^2. The question is how many such relations survive as the arguments vary.

The second polynomial is $G(n) = n(n-1)(3n-1)(3n-2)$. Expanding at a multiple of three gives

$$F(3n-3) = 9G(n). \tag{1.1}$$

Thus its kernels form the subsequence of kernels of F at positive multiples of three. This observation both shortens the counting arguments and identifies the dependence between the two random sums.

1.1 The counting theorem

Let $X \ge 3$, $I_X = [2, X] \cap \mathbb{Z}$ and $N = \lfloor X \rfloor - 1$. For $P = F$ or G set $t_P(n) = \mathrm{sf}(P(n))$ and $P(n) = t_P(n)a_P(n)^2$. For squarefree s, t put $s \odot t = \mathrm{sf}(st) = st/\gcd(s, t)^2$. This is the product in the group of positive rational square classes. We call $t_P(n) \odot t_P(m)$ the *direction* of the pair. Its value d, together with $t_P(n)$, determines $t_P(m)$.

Theorem 1.1 (Complete count)**.** *For either P, let $M^*_{4,P}(X)$ count ordered $(n_1, n_2, n_3, n_4) \in I_X^4$ with pairwise distinct entries and square $\prod_{i=1}^4 P(n_i)$. For every $\varepsilon > 0$,*

$$M^*_{4,P}(X) \ll_\varepsilon X^{5/3+\varepsilon}. \tag{1.2}$$

Every origin in I_X is allowed, regardless of the size of $a_P(n)$. The proof uses the following two estimates with moving parameters.

Theorem 1.2 (Direction and divisibility)**.** *For either quartic and every $\varepsilon > 0$, uniformly in squarefree $d > 1$,*

$$C_{P,X}(d) := \#\{(n,m) \in I_X^2 : t_P(n) \odot t_P(m) = d\} \ll_\varepsilon X^{2/3+\varepsilon}. \tag{1.3}$$

For q squarefree and $1 \le q \le T \le \max_{n\in I_X} P(n)$,

$$B_{P,X}(T;q) := \#\{n \in I_X : t_P(n) \le T,\ q \mid t_P(n)\} \ll_\varepsilon X^\varepsilon \min\{1 + X/q, \sqrt{T/q}\}. \tag{1.4}$$

The implied constants are independent of d, q, T.

The even multiplicity of each prime gives a way into the proof. Choose a largest kernel t_1 of a contributing quadruple. Each of its primes must appear in one of the other three kernels. Consequently $q = \gcd(t_1, t_j) \ge t_1^{1/3}$ for some j. For each fixed divisor q, (1.4) bounds the choices for this partner. The remaining pair has a prescribed direction. Applying the divisibility estimate to the larger of its two exclusive factors gives a second saving. Section 3 balances the two savings. A uniform norm-equation estimate suffices for this argument.

1.2 The complete random moments

Let $\epsilon(p)$ be independent random signs with probabilities $1/2, 1/2$, and extend them *completely* multiplicatively to $\mathbb{N}$. Put $S_P = \sum_{n\in I_X} \epsilon(P(n))$. Write $D_P(X) = C_{P,X}(1) - N$ for the number of ordered distinct arguments with equal kernels.

Corollary 1.3. *We have $\mathbb{E}S_P = 0$, $\mathbb{E}S_P^2 = N + D_P(X)$, and*

$$\mathbb{E}S_P^4 = 3N^2 - 2N + (6N-8)D_P(X) + M_{4,P}^*(X) = 3N^2 - 2N + O_\varepsilon(X^{5/3+\varepsilon}). \tag{1.5}$$

In fact $D_P(X) \ll \log(2X)$. With one common choice of ϵ for both polynomials, let $J = \lfloor X/3 \rfloor$. Then

$$\mathbb{E}S_F S_G = J + O(\log(2X)), \tag{1.6}$$

$$\mathbb{E}S_F^2 S_G^2 = N^2 + 2J^2 - 2J + O_\varepsilon(X^{5/3+\varepsilon}). \tag{1.7}$$

In particular $\mathbb{E}(S_F/\sqrt{N})^2(S_G/\sqrt{N})^2 \longrightarrow 11/9$.

For the fourth moments an elementary estimate $D_P(X) \ll_\varepsilon X^{2/3+\varepsilon}$ suffices. The logarithmic bound is a consequence of the theorem and its parity refinement in Luca and Walsh's *On a Diophantine equation related to a conjecture of Erdős and Graham* [15, pp. 282–283, Theorem and opening of §2]. Their integral equation is precisely the one for F after shifting the variable by one. For G, *Small roots of split quadratic congruences and fundamental units in a quartic family* already implies the weaker subpower estimate [18, Theorem 1.1 and Lemma 3.1]. Section 4 proves the logarithmic bound. Appendix A gives the fundamental-unit comparison.

1.3 Comparison with earlier work

De la Bretèche, Wang and Xu single out the untruncated four-value problem in the introduction to *Random Multiplicative Functions and Making Squares from Polynomial Values* [3, Introduction, p. 5, and Proposition 8.1]. They ask for an analogue of their quadratic square-product estimate in degree at least three when all irreducible factors have degree at most three. Theorem 1.1

gives a power saving for F and its affine restriction G by exploiting the equation $F = Q^2 - 1$. Their Theorem 1.2 already proves the marginal central limit theorem for both sums. Their passage from the truncated to the full sum uses a second-moment estimate. Convergence of the fourth moment requires further tail control.

Their Proposition 8.1 counts four-element sets under the four restrictions $a_P(n_i)^2 = P(n_i)/\operatorname{sf}(P(n_i)) \le A$, for $1 \le A \le X^5$. Let $M^*_{4,P}(X;A)$ count ordered quadruples with this cutoff on the common interval $I_X \cap [N_0(P), X]$, where $N_0(P)$ is their fixed starting point. Accounting for the 24 orderings gives

$$M^*_{4,P}(X;A) \ll_{P,\varepsilon} X^{\varepsilon} \min\Big\{A^{11/9}X^{14/9},\, X^{5/3}\Big\}.$$

The powers agree at $A = X^{1/11}$. The first is smaller below that scale. The second holds even after all four restrictions are removed.

In *Random Chowla's conjecture for Rademacher multiplicative functions*, Chinis and Shala count individually squarefree values under a no-fixed-square-divisor hypothesis [5, Proposition 3.1 and §1.4]. Pylaiev's *Random Chowla and Goldbach Conjectures* also imposes squarefreeness on each nonzero value [19, Theorem 1.5]. Both $F(n)$ and $G(n)$ are divisible by 4, so a multiplicative sign function supported on squarefree integers vanishes on these raw values. Dividing out a fixed square preserves the product class. Variable square divisors still occur, for instance when $p^2 \mid n$ for arbitrarily large primes p.

Exact equality of two products has a different orthogonality relation. It governs Steinhaus moments in Klurman, Shkredov and Xu's *On the random Chowla conjecture* [13]. In *Paucity phenomena for polynomial products*, Wang and Xu use divisors and factored congruences to count these equalities [24, Theorem 1.1 and §2]. For prime signs, a square ratio suffices. Section 3 constructs $\gg \sqrt{X}$ quadruples for F in which all three pairings have unequal products.

Erdős and Graham asked about disjoint blocks of consecutive integers in 1976 [8, p. 337] and again in 1980 [9, p. 67]. Ulas constructed infinitely many square products of four disjoint blocks of length four in *On products of disjoint blocks of consecutive integers* [22]. Bauer and Bennett's *On a question of Erdős and Graham* covers every fixed number of such blocks at least three [2, Theorem 2.2]. Skałba's count allows the number of blocks to vary [21, Theorem 2(b)]. Our upper bound fixes four starts, allows overlap and uses the largest argument as height.

2 Square parts and prescribed directions

We prove the upper bounds first for F. Restriction to $3I_X - 3 \subset I_{3X}$ transfers each of them to G, with the same exponents and an absolute change of constants. Write $t = t_F$, $a = a_F$, and $Q(n) = n^2 + 3n + 1$. The basic equations are

$$Q(n)^2 - t(n)a(n)^2 = 1, \qquad 4Q(n) + 5 = (2n+3)^2. \tag{2.1}$$

The first equation rules out $t(n) = 1$, as two positive squares cannot differ by one. Throughout the proof, divisor factors such as $\tau(m)^k$ and $k^{\omega(m)}$ for fixed k are $O_{\varepsilon,C,k}(X^{\varepsilon})$ when $1 \le m \le X^C$. We allow a smaller exponent in each invocation before absorbing finitely many such losses into X^{ε}.

For nonzero abc, Vaughan and Wooley's *Further improvements in Waring's problem* [23, Lemma 3.5] bounds the positive solutions of $ax^2 + by^2 = c$, $x, y \le H$, by $O_{\varepsilon}((|abc|H)^{\varepsilon})$. This covers our uses at polynomial height. We record the divisor and logarithmic factors for the norm equation, since the case of a single kernel uses the logarithm explicitly.

Lemma 2.1 (A quadratic norm of prescribed size)**.** *Fix C. Let $2 \le d \le X^C$ be squarefree and let $0 < |K| \le X^C$. The number of positive integer solutions of $u^2 - dv^2 = K$ with $u, v \le X^C$ is $O_C(\tau(|K|)\log(2X))$. The count for $u^2 - v^2 = K \ne 0$ is at most $2\tau(|K|)$.*

Proof. In the full ring of integers of $\mathbb{Q}(\sqrt{d})$, the principal ideal $(u+v\sqrt{d})$ has absolute norm $|K|$. There are at most $\tau(|K|)$ ideals of this norm. At a split prime the exponent e can be assigned to the two prime ideals in $e+1$ ways, and an inert or ramified prime allows at most one choice. Two generators of the same ideal with the stated norm and positive first real embedding have ratio a positive unit of norm one. If such a unit $\eta > 1$, its trace $\eta + \eta^{-1}$ is an integer at least three, so $\eta \geq (3+\sqrt{5})/2$. The possible generators lie between 1 and $2X^{3C/2}$. Their geometric spacing gives the asserted factor. In the split equation use $(u-v)(u+v) = K$. □

In particular each fixed kernel has $O(\log(2X))$ preimages by (2.1) and strict monotonicity of Q. Luca and Walsh give the stronger absolute bound of three preimages over the entire positive range [15, p. 282]. We retain the elementary height bound in the proof of Theorem 1.1. Its constant is uniform, since $t(n) \ll X^4$ and $a(n) \ll X^2$.

2.1 The tail of the square part

Write $n+i = s_i b_i^2$, $0 \leq i \leq 3$, with s_i squarefree. For $i \neq j$ the integers b_i, b_j are coprime, since a common prime p would force $p^2 \mid i-j$. A prime dividing more than one s_i is either 2 or 3 and occurs in at most two of them. Consequently

$$\prod_{i=0}^{3} s_i = e^2 t(n), \qquad a(n) = e \prod_{i=0}^{3} b_i, \qquad e \mid 6. \tag{2.2}$$

The finite factor e matters; the individual square parts need not multiply to $a(n)$.

Lemma 2.2. *For $1 \leq U \leq X^{1/3}$,*

$$\#\{n \in I_X : a_P(n) > 6U\} \ll_\varepsilon X^\varepsilon (X/U + \sqrt{X} + U^2) \ll_\varepsilon X^{1+\varepsilon}/U \quad (P = F, G).$$

Proof. For F, if some $b_i > U$, sum $O(X/b^2+1)$ over $U < b \leq \sqrt{X+3}$ for the congruence $n \equiv -i \bmod b^2$. This costs $O(X/U + \sqrt{X})$. The individual factors are linear, so the sum runs only up to $O(\sqrt{X})$.

If every $b_i \leq U$, then (2.2) forces $\prod b_i > U$ for each counted origin. We use the short divisor interval of Cutter, Granville and Tucker, *The Number of Fields Generated by the Square Root of Values of a Given Polynomial* [6, §4, pp. 76–77]. They choose the least integer $m > y$ whose prime factors are at most y and whose square divides the polynomial value. This gives $m \leq y^2$. Here multiply successive b_i until their product D first exceeds U. It satisfies $U < D \leq U^2$. For fixed D, distributing its prime powers among the four positions gives at most $4^{\omega(D)}$ coprime assignments. Each prescribes a single residue modulo D^2. Summing $4^{\omega(D)}(X/D^2+1)$ gives $O_\varepsilon(X^\varepsilon(X/U+U^2))$. For G, if $a_G(n) > 6U$, then $a_F(3n-3) = 3a_G(n) > 18U > 6U$. The injection $n \mapsto 3n-3$ thus permits the estimate for F at height $3X$ with the *same* U, which satisfies $U \leq (3X)^{1/3}$. □

2.2 A uniform bound for a direction

For a pair (n,m) of direction d, put $g = \gcd(t(n), d)$, $a = a(n)$, $b = a(m)$. We have $g \mid d$ and $t(m) = dt(n)/g^2$. Eliminating $t(n)$ from (2.1) gives

$$(gaQ(m))^2 - d(bQ(n))^2 = g^2a^2 - db^2. \tag{2.3}$$

For squarefree $d > 1$ the right side is nonzero. An occurring d is at most $\max F(n)^2 \ll X^8$, so every integer in (2.3) has polynomial size in X, with an absolute exponent.

Restrict first to $a, b \leq 6X^{1/3}$. There are $O(X^{2/3})$ choices for a, b and at most $\tau(d)$ choices for g. For each choice the two coordinates of a norm solution recover m, n uniquely by monotonicity.

Lemma 2.1 bounds the number of solutions by $O_\varepsilon(X^\varepsilon)$, uniformly even when d has many prime factors. If either square part is larger, Lemma 2.2 removes $O_\varepsilon(X^{2/3+\varepsilon})$ possible origins in that position. Its partner then belongs to one fixed kernel and has $O(\log(2X))$ choices. This proves (1.3).

The same argument gives

$$D_P(X) \ll_\varepsilon X^{2/3+\varepsilon}. \tag{2.4}$$

Indeed, at $d = 1$ we have $g = 1$, and $a = b$ would force $F(m) = F(n)$, hence $m = n$. Off the diagonal $a^2 - b^2 \neq 0$, so the split case of Lemma 2.1 applies. This elementary estimate is the only equal-kernel input used in the proof of (1.2).

2.3 Divisibility of a small kernel

For (1.4), the congruence $q \mid F(n)$ has at most $4^{\omega(q)}$ residue classes when q is squarefree. This gives $O_\varepsilon(X^\varepsilon(1 + X/q))$.

Suppose now that $q \mid t(n) \leq T$. For each $p \mid q$ choose one of the s_i divisible by p. This splits q into pairwise coprime factors $q_0q_1q_2q_3$ with $q_i \mid s_i$, in at most $4^{\omega(q)}$ ways. Write $s_i = q_ir_i$. Equation (2.2) gives $\prod_i r_i \leq 36T/q$. The two smallest r_i, r_j therefore have product at most $6\sqrt{T/q}$. The two positions have at most six choices, and the number of ordered positive pairs of product at most V is at most $V(1 + \log V)$. Thus there are $O_\varepsilon(X^\varepsilon\sqrt{T/q})$ choices including the allocation of q.

For fixed $i < j, s_i, s_j$, subtraction gives $s_jb_j^2 - s_ib_i^2 = j - i$. Write $s_is_j = h^2d_0$ with d_0 squarefree. Multiplication by s_j yields

$$(s_jb_j)^2 - d_0(hb_i)^2 = s_j(j - i) \neq 0.$$

Lemma 2.1, including $d_0 = 1$, leaves $O_\varepsilon(X^\varepsilon)$ origins. This proves the second bound in (1.4). A bound T above the largest value can always be replaced by that largest value. If $q > T$, the count is zero.

3 Counting four distinct origins

We give the argument for either P, using the two uniform estimates just proved. Write $t_i = t_P(n_i)$. If $t_1t_2t_3t_4$ is a square, we can permute the arguments so that t_1 is maximal and

$$q = \gcd(t_1, t_2) \geq t_1^{1/3}, \qquad d = t_1 \odot t_2 = t_3 \odot t_4. \tag{3.1}$$

In fact t_1 divides the product of its three gcds with the other kernels. Permuting costs at most an absolute factor. The configurations with $d = 1$ cost at most $D_P(X)^2$ for each ordering, since both pairs have distinct origins. By (2.4) these contribute $O_\varepsilon(X^{4/3+\varepsilon})$.

Fix n_1 and $q \mid t_1$, and let $T \leq t_1 < 2T$, $S \leq t_2 < 2S$ be dyadic, with $S \leq T$. There are $O_\varepsilon(X^\varepsilon)$ choices of divisor and scale for each first origin. We retain only actual partners satisfying $\gcd(t_1, t_2) = q$. For their number one may relax this to $q \mid t_2$, so (1.4) gives

$$\ll_\varepsilon X^\varepsilon A, \qquad A = \min\{1 + X/q, \sqrt{S/q}\}. \tag{3.2}$$

Absolute factors from dyadic endpoints are absorbed in the implied constants. If a partner exists then $q \leq 2S$.

For each such n_2 the direction $d > 1$ is now fixed. Write $t_3 = hu$, $t_4 = hv$ with $h = \gcd(t_3, t_4)$. Then $uv = d$. There are at most $\tau(d)$ ordered choices of u, v, and one of them is at least $\sqrt{d}$. Suppose it is u. Since $u \mid t_3 \leq 2T$, (1.4) bounds the choices for n_3. Once n_3 is chosen,

$t_4 = d \odot t_3$ is fixed, leaving only $O(\log(2X))$ choices for n_4. The other ordering gives the same bound. Together with (1.3), the number of completions is

$$\ll_\varepsilon X^\varepsilon C, \qquad C = \min\{X^{2/3},\, 1 + X/\sqrt{d},\, \sqrt{T/\sqrt{d}}\}. \tag{3.3}$$

For each retained partner the exact gcd gives $d = t_1 t_2/q^2 \asymp TS/q^2$. Thus the completion bound is uniform within the chosen ranges even though d varies.

Balancing the two choices. If $q \geq X$, then $A \leq 2$ and we use $C \leq X^{2/3}$. If $q < X$ and $d \geq X^2$, then $C \leq 2$. Here $S \leq T \leq t_1 \leq q^3$ by (3.1), so $A \ll \min(X/q, q) \ll \sqrt{X}$. These are the two places where the constant terms in (3.2)–(3.3) must be kept.

It remains that $q < X$ and $d < X^2$. Set $z = T/q$. First use the kernel-size bound for the partner and the congruence bound for the completion:

$$AC \ll \sqrt{S/q}\,\frac{Xq}{\sqrt{TS}} = Xz^{-1/2}.$$

Next take the geometric mean of the two bounds for A and use the kernel-size bound for C:

$$AC \ll (X/q)^{1/2}(S/q)^{1/4}\frac{T^{1/2}q^{1/2}}{(TS)^{1/4}} = X^{1/2}z^{1/4}.$$

Taking their weighted geometric mean eliminates z, giving

$$AC \ll (Xz^{-1/2})^{1/3}(X^{1/2}z^{1/4})^{2/3} = X^{2/3}.$$

Thus each first origin costs $O_\varepsilon(X^{2/3+\varepsilon})$ after the divisor and scale sums. At the formal scales $T = S = X^{4/3}$, $q = X^{2/3}$, the two budgets A and C are both of order $X^{1/3}$. This identifies where the estimates meet without assuming such parameters occur with any prescribed frequency. Summing over at most X first origins proves (1.2).

A family with overlapping blocks. The use of distinct origins allows their intervals of four consecutive integers to overlap. This gives an elementary lower bound on the same count for F. Since $\mathrm{sf}(F(u)F(u+1)) = \mathrm{sf}(u(u+4))$, put $v = u(u+4)$. The identity $v + 4 = (u+2)^2$ gives

$$\mathrm{sf}(F(u)F(u+1)) = \mathrm{sf}(F(v)F(v+1)).$$

For $u \geq 2$ the four origins $u, u+1, v, v+1$ are distinct. The least argument u identifies the set. Counting $2 \leq u \leq \lfloor\sqrt{X+3}\rfloor - 2$, for which $v + 1 \leq X$, and allowing all permutations gives $24(\lfloor\sqrt{X+3}\rfloor - 3)$ ordered quadruples for $X \geq 13$. In fact none of the three pairings yields an exact equality of products. By strict monotonicity of F, the only possible equality would be $F(u)F(v+1) = F(u+1)F(v)$. But $F(w+1)/F(w) = (w+4)/w$ decreases strictly with $w > 0$. Thus the lower bound persists after discarding *every* quadruple that solves an exact product equality. The blocks at adjacent starts overlap in three positions. The gap between $\sqrt{X}$ and the upper bound leaves the optimal exponent open.

3.1 What the repeated indices contribute

For independent fair signs on primes, $\mathbb{E}\prod_i \epsilon(P(n_i))$ is exactly the indicator that $\prod_i P(n_i)$ is a square. Each prime of odd total valuation contributes an independent sign of mean zero. This gives $\mathbb{E}S_P = 0$ and $\mathbb{E}S_P^2 = N + D_P(X)$.

For the fourth moment the three partitions into pairs each give N^2 tuples. Their only intersections are the N constant tuples, each counted three times. The remaining configurations

with a repeated index have multiplicities $3+1$ or $2+1+1$. The first case has $4D_P(X)$ choices, by marking the singleton position. In the second case choose the two positions of the double index in six ways. The singleton origins form an ordered equal-kernel pair, and the repeated origin has $N-2$ choices. Adding $M^*_{4,P}(X)$ gives the exact identity (1.5). In particular all terms in the excess over $3N^2-2N$ are nonnegative.

For example, at $X=28$ there are $N=27$ origins and $D_P(X)=0$ for both polynomials. Directly testing all $\binom{27}{4}$ four-element subsets gives 28 square products for F and 2 for G. Thus the common diagonal contribution 2133 increases by $24\cdot 28$ and $24\cdot 2$, giving fourth moments 2805 and 2181. To see the effect of a genuine repetition of the kernel, restrict F to the four arguments $2, 3, 33, 1680$. Their kernels are $30, 10, 39270, 39270$, so $D=2$ and $M^*_4=0$ on this set. The fourth moment is $3\cdot 4^2-2\cdot 4+(6\cdot 4-8)\cdot 2=72$.

This proof also covers arbitrary deterministic real weights $|b_n|\le 1$. If $S_b=\sum_{n\in I_X} b_n\epsilon(P(n))$, then

$$\mathbb{E}S_b^4=3\Big(\sum_n b_n^2\Big)^2-2\sum_n b_n^4+O_\varepsilon(X^{5/3+\varepsilon}),\qquad \Big|\mathbb{E}S_b^2-\sum_n b_n^2\Big|\le D_P(X). \tag{3.4}$$

Indeed, after summing the paired tuples exactly, bound each remaining weight product by one. For the indicator of any subset of size at least $X^{5/6+\delta}$, $\delta>0$ fixed, its sum divided by the square root of the subset size has fourth moment tending to three, uniformly over the subsets.

3.2 Using the same signs for the two quartics

For F, the two index sets giving S_F, S_G are $A=I_X$ and $B=\{3m-3 : m\in I_X\}$, by (1.1). They have N elements each, and $|A\cap B|=J=\lfloor X/3\rfloor$. In the mixed second moment each common index contributes one. All remaining contributing pairs belong to the $D_F(3X)$ distinct equal-kernel pairs.

For the mixed fourth moment, use A, A, B, B in that order. The three possible pairings supply N^2, J^2, J^2 tuples. Their triple intersection and all three pairwise intersections consist of the J common constant tuples. The number of other contributing tuples is at most $(6|I_{3X}|-8)D_F(3X)+M^*_{4,F}(3X)$, by embedding them in the full fourth-moment count at height $3X$. This proves (1.7) and, with the equal-kernel estimate below, (1.6). In particular the fraction $J/N\to 1/3$ accounts for the additional $2/9$ in the mixed fourth moment. At $X=28$ the mixed second moment is 9, and the mixed fourth moment is 1065, of which 873 comes from the three pairings and 192 from the remaining configurations. A joint limit law would require additional information beyond these moments.

4 Equal kernels and the parity of the Pell exponent

Luca and Walsh singled out the kernel 39270 in their conjecture on double representations [15, p. 282]. Bauer and Bennett use the corresponding pair of starting points explicitly [2, §4]. Its two values are

$$F(33)=39270\cdot 6^2,\qquad F(1680)=39270\cdot 14268^2.$$

Both indices are multiples of three, so $G(12)$ and $G(561)$ give the same kernel. The theorem of Luca and Walsh gives a height bound for all such pairs without assuming the conjectural classification.

Corollary 4.1 (Height bound after Luca and Walsh)**.** *With $L_0=\log(3+\sqrt{8})$, the ordered distinct equal-kernel counts satisfy*

$$D_F(X)\le (2/L_0)\log X+O(1),\qquad D_G(X)\le (1/L_0)\log X+O(1).$$

The constants multiplying $\log X$ are upper bounds.

Proof. Fix a squarefree $t > 1$. In the integer Pell equation $x^2 - ty^2 = 1$ write $\eta_t = x_t + y_t\sqrt{t}$ for the least unit above one with positive integer coordinates. The positive solutions are the powers η_t^j. Indeed division by a suitable power leaves a unit in $[1, \eta_t)$ with integer coordinates and positive conjugate, which must be one. Set $T_j(x_t) = (\eta_t^j + \eta_t^{-j})/2$. At an origin of kernel t, (2.1) gives

$$T_j(x_t) = Q(n) = (n+1)^2 + (n+1) - 1.$$

This is equation (2) of Luca and Walsh with $x = n+1$ and the same minimal *integer-coordinate* solution of the Pell equation. For all t they prove at most three solutions, and for $t > C_1$, where C_1 is an absolute computable constant, at most two. At the start of their proof they record the parity refinement: there is at most one even index for any t, and at most one odd index when $t > C_1$ [15, Theorem, pp. 282–283, and §2].

The finitely many $t \le C_1$ contribute $O(1)$ ordered pairs. For each remaining t, an equal-kernel pair needs one even exponent $j = 2h$ and one odd exponent. The even origin has at most one partner. Since $T_{2h}(x_t) = 2T_h(x_t)^2 - 1$, the second identity in (2.1) gives

$$y^2 - 8z^2 = 1, \qquad y = 2n + 3, \quad z = T_h(x_t). \tag{4.1}$$

The positive solutions have $y + z\sqrt{8} = (3 + \sqrt{8})^r$, $r \ge 1$: $3 + \sqrt{8}$ is the smallest positive solution and division by its powers gives them all. For $n \le X$, $(3 + \sqrt{8})^r < 2y \le 4X + 6$. Each exponent r determines at most one even origin, hence at most two ordered pairs. This proves the first inequality.

For G, use $F(3n - 3) = 9G(n)$. In (4.1) the coordinate $y = 6n - 3$ is divisible by three and at most $6X - 3$. The first coordinates of $(3 + \sqrt{8})^r$ satisfy $y_0 = 1$, $y_1 = 3$, $y_{r+2} = 6y_{r+1} - y_r$, so precisely the odd r give $3 \mid y_r$. Only half the exponents up to $\log(12X)/L_0$ can occur. Each supplies at most two ordered pairs, proving the second inequality. □

5 Reconstructing a pair from its product class

For each squarefree d, let $U(d)$ be the number of unordered pairs of distinct indices in I_X with direction d. Let $\mathcal{D} = \{d : U(d) > 0\}$ and $K = \binom{N}{2}$. The directions with multiplicity at least two measure the loss of information when a pair is replaced by its product class.

Cutter, Granville and Tucker [6, Theorems 1A–1C] and Poonen [16, Theorem 3.5 and §9] study the image of *individual* polynomial values in square classes. Poonen assumes *abc* when the squarefree polynomial part has degree greater than three. Krumm studies the residue classes of kernels of rational values [14, §1]. Here a class labels a pair of integral arguments of bounded height. The collision identity below holds in every abelian group of exponent two. The power saving comes from Theorem 1.1.

Proposition 5.1. *One has the exact identity*

$$\sum_d U(d)(U(d) - 1) = \tfrac{1}{4} M_{4,P}^*(X) + (N - 2) D_P(X). \tag{5.1}$$

The probability that the direction of a uniformly sampled unordered pair admits a second representation is $O_\varepsilon(X^{-1/3+\varepsilon})$. Also $0 \le K - |\mathcal{D}| \ll_\varepsilon X^{5/3+\varepsilon}$.

Proof. The left side counts ordered lists of two different unordered pairs with the same direction. If the pairs are disjoint there are four orderings of the two pairs' entries for each list, giving the first term on the right. If they meet, their unique common index cancels from the product. The other two indices are an ordered distinct equal-kernel pair and the common index has $N - 2$ choices. This gives the second term. For a direction of multiplicity $u \ge 2$, both u and $u - 1$ are at most $u(u - 1)$. Sum and use Theorem 1.1 and (2.4). □

Here is the resulting signed identity. Let $\lambda(n) = (-1)^{\Omega(n)}$, with prime factors counted with multiplicity, and $c_{P,X} = N^{-1} \sum_{n \in I_X} \lambda(P(n))$. For $N \geq 2$,

$$c_{P,X}^2 = \frac{N + 2\sum_d U(d)\lambda(d)}{N^2} = \frac{1}{|\mathcal{D}|} \sum_{d \in \mathcal{D}} \lambda(d) + O_\varepsilon(X^{-1/3+\varepsilon}). \tag{5.2}$$

Indeed, replacing $\sum U(d)\lambda(d)$ by $\sum_{d \in \mathcal{D}} \lambda(d)$ costs at most $K - |\mathcal{D}|$, and $2K/N^2 = 1 - 1/N$. The estimate controls multiplicity. A signed estimate of the last sum is a separate arithmetic question. For example, square classes $p_i q_i$ built from disjoint pairs of distinct primes have no nontrivial pair collisions, while every class has Liouville sign $+1$.

5.1 Forgetting a fixed set of square-class directions

Let μ be the law of $t_P(n)$ for a uniform origin. Its overlap with its translate by d satisfies, for $d > 1$,

$$\mathcal{R}(d) = \sum_s \min(\mu(s), \mu(s \odot d)) \leq C_{P,X}(d)/N \ll_\varepsilon X^{-1/3+\varepsilon}.$$

For integer multiplicities the minimum of two positive counts is at most their product. A related uniform estimate holds when the origin has probability proportional to $1/n$. To see this, for two classes expand the minimum of their masses into the upper bound given by the sum, over pairs, of the minima of their point masses. The elementary inequality used here is $\min(\sum_i u_i, \sum_j v_j) \leq \sum_{i,j} \min(u_i, v_j)$ for nonnegative weights. Before normalization, a pair whose larger origin lies in $(2^{j-1}, 2^j]$ costs at most 2^{1-j}. Estimate (1.3) bounds the number of such pairs by $O_\varepsilon(2^{j(2/3+\varepsilon)})$, uniformly in $d > 1$. Summing with $\varepsilon < 1/3$ and dividing by $\sum_{2 \leq n \leq X} 1/n$ gives $\mathcal{R}_{\log}(d) \ll 1/\log(2X)$.

For example, suppose the observed label is the class of $t_P(n)$ modulo a subgroup H of dimension r over $\mathbb{F}_2$. In each coset the optimal error for predicting $\lambda(t_P(n))$ is the smaller of the positive and negative masses. Using the same minimum inequality and counting each unordered cross-sign pair twice gives the bound

$$\frac{1}{2} \sum_{\substack{d \in H \\ \lambda(d) = -1}} \mathcal{R}(d).$$

It is $O_\varepsilon(2^r X^{-1/3+\varepsilon})$ for uniform origins, and $O(2^r/\log(2X))$ for logarithmic origins. The subgroup may be prescribed separately at each X.

6 The size and common factors of a direction

Two independently chosen origins have kernels $t = t_P(n)$ and $t' = t_P(m)$. Write $g = \gcd(t, t')$, so their direction is $d = tt'/g^2$. The following estimates concern ordinary uniform sampling with replacement.

The qualitative limit also follows from Kabluchko and Marynych's *Divisibility properties of polynomial expressions of random integers* [11, Proposition 2.1 and Theorem 3.1]. In $\mathbb{Z}[x, y]$ the polynomials $P(x)$ and $P(y)$ have no common factor of positive degree. Their theorem gives tightness of the ordinary gcd, which is a multiple of g. For finitely many primes the profinite Haar limit gives the parities of the valuations, since the polynomial zero sets have Haar measure zero. Tightness removes the remaining primes. Omitting the first integer in either sampling interval changes probabilities by $O(1/X)$. Below we compute the local parameters and give a tail estimate uniform in R.

Proposition 6.1. *For $1 \le R \le \sqrt{X}$ and every $\varepsilon > 0$,*

$$\#\{(n,m) \in I_X^2 : g > R\} \ll_\varepsilon X^2 R^{-1+\varepsilon}.$$

Let $\rho_P(p)$ be the probability of odd valuation of $P(x)$ for Haar-uniform $x \in \mathbb{Z}_p$. For fixed squarefree e,

$$\lim_{X\to\infty} \mathbb{P}(g = e) = \prod_{p\mid e} \rho_P(p)^2 \prod_{p\nmid e} (1-\rho_P(p)^2), \qquad \begin{array}{c|ccc} & 2 & 3 & p \ge 5 \\ \hline \rho_F(p) & 2/3 & 2/3 & 4/(p+1) \\ \rho_G(p) & 2/3 & 1/2 & 4/(p+1). \end{array} \tag{6.1}$$

Proof. If a prime $p > R$ divides g, it lies below $3X+3$, and the two origins lie in at most 4^2 pairs of residues modulo p. The sum of $O((X/p+1)^2)$ for $R < p \le 3X+3$ is $O(X^2/R)$. If all prime factors of g are at most R, multiply successive factors until obtaining $R < e \le R^2 \le X$. The CRT gives $O(16^{\omega(e)}X^2/e^2)$ pairs. Indeed, for $0 < \varepsilon < 1$ the divisor bound and an integral comparison give

$$\sum_{e>R} \frac{16^{\omega(e)}}{e^2} \ll_\varepsilon \sum_{e>R} e^{-2+\varepsilon} \ll_\varepsilon R^{-1+\varepsilon}.$$

This proves the stated tail estimate. Larger ε follow by weakening the bound.

For $p \ge 5$ the four roots are distinct and simple for each quartic. One root contributes $(1-1/p)\sum_{j \text{ odd}, j\ge1} p^{-j} = 1/(p+1)$. At 2, among four consecutive integers one even factor has valuation exactly one and the other is Haar-uniform among multiples of four. Their total valuation is odd with probability 2/3. At 3, for F, the two factors divisible by 3 in the branch $n = 3k$ give parity $v_3(k(k+1))$; it is odd with probability 1/2. In either other branch the unique multiple of 3 has odd valuation with probability 3/4. Averaging gives 2/3. By (1.1), G selects the first branch at 3 and an invertible affine substitution at every other prime.

For finitely many primes, truncate valuations at a fixed power, apply the CRT to the two independent origins and let the truncation grow. A fixed p-adic root has measure zero and the discarded root neighborhoods shrink to finitely many points. Thus divisibility of g at these primes has the product law with parameters $\rho_P(p)^2$. A new prime beyond a cutoff R implies $g > R$, whose probability tends uniformly to zero as $R \to \infty$. The infinite product converges since $\sum_p \rho_P(p)^2 < \infty$. □

Proposition 6.2. *For every fixed $0 < \delta \le 8$ and every $\varepsilon > 0$,*

$$\#\{(n,m) \in I_X^2 : t_P(n) \odot t_P(m) \le X^{8-\delta}\} \ll_{\delta,\varepsilon} X^{2-\min(\delta/6,\,1/3)+\varepsilon}. \tag{6.2}$$

Proof. Each polynomial satisfies $P(n) \ge n^4$ for $n \ge 2$. Combine the loss from a short argument and the loss from its square part in the single quantity $W(n) = (X/n)\sqrt{a_P(n)} \ge 1$. We first show

$$\#\{n \in I_X : W(n) > z\} \ll_\varepsilon X^{1+\varepsilon}/z \qquad (1 \le z \le X^{1/3}). \tag{6.3}$$

The origins $n \ll X/z$ already satisfy this count. On a dyadic interval $U < n \le 2U$ above X/z, the event implies $a_P(n) > (zU/X)^2$. Apply Lemma 2.2 at height $2U$ with threshold $\min((zU/X)^2/6, (2U)^{1/3})$, using the trivial bound when the parameter is below one. This costs

$$O_\varepsilon\left(X^\varepsilon\left(\frac{X^2}{z^2U} + U^{2/3}\right)\right).$$

The first terms sum to $O_\varepsilon(X^{1+\varepsilon}/z)$, the second to $O_\varepsilon(X^{2/3+\varepsilon})$, proving (6.3). For independent n, m, a dyadic decomposition in $W(n)$ now gives

$$\#\{(n,m) : W(n)W(m) > z\} \ll_\varepsilon X^{2+\varepsilon}/z, \qquad 1 \le z \le X^{1/3}.$$

Indeed the terms with $W(n) > z$ cost this bound. For $v \le W(n) < 2v \le 2z$, multiply the two bounds at thresholds comparable to v and $\max(1, z/(2v))$, using the trivial count at the endpoint one. Absorb the logarithm and the two individual divisor losses in ε.

Outside this event and $g > z$, the factorization of the direction gives

$$d = \frac{P(n)P(m)}{a_P(n)^2 a_P(m)^2 g^2} \ge \frac{X^8}{(W(n)W(m))^4 g^2} \ge X^8/z^6.$$

Take $z = \frac{1}{2}X^{\min(\delta/6,1/3)}$ for large X and use Proposition 6.1. This proves (6.2). □

In particular the average in (5.2) can be restricted to $d > X^{8-\delta}$, normalizing by the number of such directions, with error $O_{\delta,\varepsilon}(X^{-\min(\delta/6,1/3)+\varepsilon})$. Every excluded represented direction costs at least one pair and $|\mathcal{D}| \sim N^2/2$.

There is also an exact way to retain signed information at a prescribed common divisor. Put $A(q) = N^{-1}\sum_{q|t_P(n),\, n\in I_X} \lambda(P(n))$ for squarefree q. Then $\mathbb{E}_{n,m}\mathbf{1}_{q|g}\lambda(d) = A(q)^2$, and

$$\mathbb{E}_{n,m}\mathbf{1}_{g=q}\lambda(d) = \sum_{(r,q)=1} \mu(r)A(qr)^2,$$

where only squarefree r need be included. This is ordinary Möbius inversion on the squarefree divisors of g. The local law (6.1) gives their unsigned frequencies.

7 Reading the class at large primes

A direction can be observed one bit at a time. For a single origin use $V = P(n)$. For an unordered pair of distinct origins use $V = P(n)P(m)$. At a prime p read the one Legendre symbol (V/p). On distinct represented classes the random panel is a family of hash functions with pairwise collision probability at most $(1 + o(1))2^{-k}$. This is the collision principle of Carter and Wegman's *Universal Classes of Hash Functions* [4, pp. 144–145], with an asymptotic error. The ambiguity between objects that already represent the same class must be counted separately.

Proposition 7.1. *Let $Y = \exp(C_0(\log X)^2)$ with $C_0 > 0$ a sufficiently large absolute constant. Sample $k = O(\log X)$ primes independently and uniformly, with replacement, from $(Y, 2Y]$. Choose a uniform object independently of the primes. Write K_0 for the number of possible objects. The probability, over both the panel and the object, that a second object gives the same observations is at most*

$$e_X + (K_0 - 1)2^{-k}(1 + o(1)), \qquad \begin{array}{l|cc} & K_0 & e_X \\ \hline \textit{one origin} & N & D_P(X)/N \\ \textit{one unordered pair} & \binom{N}{2} & O_\varepsilon(X^{-1/3+\varepsilon}). \end{array} \tag{7.1}$$

The $o(1)$ is uniform for k in any fixed range $k \le A\log X$. If $k - \log_2 K_0 \to +\infty$, the probability of unique recovery tends to one under the joint sampling. If $k - \log_2 K_0 \to -\infty$, the optimal success probability for a uniform object tends to zero for every fixed panel of these primes.

Proof. All primes in the panel exceed every prime factor of either object's value for large X. For two different classes let $d = \mathrm{sf}(VV') > 1$. The two symbols agree exactly when $\chi(p) = 1$, where χ is the primitive quadratic character of the positive fundamental discriminant of $\mathbb{Q}(\sqrt{d})$. Its conductor $D \le 4d \ll X^{16}$, including the pair experiment. We use the one-sided estimate

$$\frac{1}{\pi(2Y) - \pi(Y)} \sum_{Y<p\le 2Y} \chi(p) \;\le\; C_1 \exp(-c\sqrt{\log Y}). \tag{7.2}$$

A possible exceptional real zero has a favorable sign here. We include the argument to clarify uniformity in the changing conductor.

Use the truncated explicit formula for a primitive nonprincipal character, the classical Dirichlet zero-free region with at most one simple real exception, and the zero count on intervals of length one [7, Chapters 14, 16, 19–20]. A form of the formula uniform in the conductor, including the constant arising from low zeros, is given in [12, §11.1, Lemma 11.1 and the following formula, and §11.2, Theorem 11.2]. Take $H = \exp(\sqrt{\log Y})$. Subtract the formulas at Y and at $z \in [Y, 2Y]$, using integer endpoints with an $O(\log^2(DY))$ rounding error. The constant cancels. For a zero ρ the summand is $-(z^\rho - Y^\rho)/\rho$. Apart from the possible exception, all zeros with $|\Im\rho| \le H$ have real part at most $1 - c_1/\log(D(H+2))$. The conductor range gives $\log(D(H+2)) \ll \sqrt{\log Y}$. For zeros with $|\Im\rho| \le 1$, use the integral of $u^{\rho-1}$ from Y to z, so a zero close to zero causes no loss. For the other zeros the sum of $1/|\Im\rho|$ is $O(\log^2(D(H+2)))$. The truncation error is $O(YH^{-1}\log^2(DY))$. A real exceptional zero β contributes $-(z^\beta - Y^\beta)/\beta \le 0$. It follows uniformly in z that

$$\sum_{Y<n\le z} \Lambda(n)\chi(n) \le C_2 Y \exp(-c_2\sqrt{\log Y}).$$

Removing proper prime powers costs $O(\sqrt{Y}\log^2 Y)$. Write $B(z) = \sum_{Y<p\le z} \chi(p)\log p$. In partial summation,

$$\sum_{Y<p\le 2Y} \chi(p) = \frac{B(2Y)}{\log(2Y)} + \int_Y^{2Y} \frac{B(u)}{u\log^2 u}\,du.$$

Both weights are positive, so the upper bound on $B(u)$ suffices. The ordinary prime number theorem gives (7.2) with constants independent of d, X.

Consequently two distinct classes survive k independent probes together with probability at most $2^{-k}(1 + O(e^{-c\sqrt{\log Y}}))^k = 2^{-k}(1 + o(1))$. An origin with a competing representative of exactly its own class has probability at most $D_P(X)/N$; for unordered pairs use Proposition 5.1. On the complement, sum the distinct-class bound over competitors. This proves (7.1). The upper recovery statement follows by using just $O(\log X)$ of the probes if necessary. Conversely a fixed panel has at most 2^k observable words, so any decoder has uniform success at most $2^k/K_0$. □

For a panel $\mathcal{P}$, let $e(\mathcal{P})$ be the proportion of objects with a competing match. Above the threshold, $\mathbb{E}_{\mathcal{P}} e(\mathcal{P}) = o(1)$, hence $e(\mathcal{P}) \to 0$ in probability over panels. Unique recovery can be tested by enumerating the candidates. The threshold concerns identifiability and places no bound on the computational cost of decoding.

In *Simultaneous quadratic probes: reconstruction thresholds and marked Poisson limits* [17, Theorem 1.1], a prime can return four separate symbols, one for each affine form, and divisibility can erase the row. Here the primes are much larger and each returns just the sign of the product. The common arithmetic input to the two recovery questions in (7.1) is the number of objects that agree before any observation is made. In particular knowledge of the direction can usually identify a pair, while (5.2) still requires the Liouville signs of those directions.

A Comparison with fundamental units in the full ring

The proof of Theorem 1.1 uses the elementary estimate (2.4), and Corollary 4.1 gives a logarithmic refinement. This appendix records a separate deduction from fundamental units for comparison with the earlier quartic family. There is an independent bound for G in *Small roots of split quadratic congruences and fundamental units in a quartic family* [18, Theorem 1.1 and Lemma 3.1]. With $k = n - 1$, its polynomial $D(k) = k(k+1)(3k+1)(3k+2)$ is $G(n)$. Its

prescribed unit increases strictly with k. Outside $\exp(O((\log(2X))^{2/3}))$ exceptional indices it is the fundamental unit in the full ring of integers of the field of the kernel. Thus a distinct equal-kernel pair contains an exceptional index. The spacing in Lemma 3.1 of that paper gives $O(\log(2X))$ partners per index, yielding $D_G(X) \ll \exp(O((\log(2X))^{2/3}))$. An exceptional power can occur without another origin in the same kernel. The fundamental-unit exceptional set and the set of equal-kernel pairs measure different phenomena.

The same Chebyshev curves also give the subpower bound for F by a different route. Among origins of fixed kernel at most one has $j = 1$. The even j are controlled by (4.1). For odd $j \geq 3$ with a prime divisor $\ell \leq L$, set $x = 2T_{j/\ell}(x_t)$, $y = 2n + 3$ and $D_\ell(w) = 2T_\ell(w/2)$. Then $y^2 = 2D_\ell(x) + 5$. At $\ell = 3$ this is the separable cubic $2x^3 - 6x + 5$, so Siegel's theorem gives finitely many integral points [20]. At primes $\ell \geq 5$, equations (4.1)–(4.2) and Corollary 4.3 of [18] give at most $\exp(C\ell^2)$ points: the map $(x, y) \mapsto (2x, 2^{(\ell-1)/2}y)$ embeds the solutions in the monic integral equation counted there. This bound, uniform in ℓ, specializes Alpöge's descent [1, Theorem 1.1 and §3] with Evertse's bound for unit equations [10]. It applies to all integral y.

For the remaining odd exponents $j > L$, convexity in the defining formula gives $T_j(x_t) \geq x_t^j$. Thus $x_t \ll X^{2/L}$, and each x_t determines $t = \mathrm{sf}(x_t^2 - 1)$. Using the elementary $O(\log(2X))$ bound per fibre, and taking $L = \max(3, \lfloor(\log(2X))^{1/3}\rfloor)$, again gives an upper bound $\exp(O((\log(2X))^{2/3}))$ for the pairs. The logarithmic bounds of Corollary 4.1 use the additional parity information of Luca and Walsh.

Assistance and reproducibility. OpenAI Codex assisted with the mathematical arguments, bibliographic checks, writing and finite computations. The author retains responsibility for the manuscript. The accompanying archive `Square_Class_Collisions_and_Complete_Fourth_Moments_sources.zip` contains the LaTeX source and the exact checks. From its root, run `python3 checks/reproduce.py` (Python 3.10 or later). The SHA-256 digest of `checks/SHA256SUMS` begins with `93139cc6c1c235d47caf`. The program verifies the files, recomputes the examples and checks the exponent bounds over the rationals.

References

[1] L. Alpöge, *Note on a theorem of Professor X.*, 2021. arXiv:2109.14328v1. doi: 10.48550/arXiv.2109.14328.

[2] M. Bauer and M. A. Bennett, *On a question of Erdős and Graham*, L'Enseignement Mathématique (2) **53** (2007), 259–264. doi: 10.5169/seals-109547.

[3] R. de la Bretèche, V. Y. Wang and M. W. Xu, *Random Multiplicative Functions and Making Squares from Polynomial Values*, 2026. arXiv:2607.06398v1. doi: 10.48550/arXiv.2607.06398.

[4] J. L. Carter and M. N. Wegman, *Universal Classes of Hash Functions*, Journal of Computer and System Sciences **18** (1979), 143–154. doi: 10.1016/0022-0000(79)90044-8.

[5] J. Chinis and B. Shala, *Random Chowla's conjecture for Rademacher multiplicative functions*, Transactions of the American Mathematical Society **378** (2025), 8025–8053. doi: 10.1090/tran/9457. arXiv:2409.05952v2.

[6] P. Cutter, A. Granville and T. J. Tucker, *The Number of Fields Generated by the Square Root of Values of a Given Polynomial*, Canadian Mathematical Bulletin **46** (2003), 71–79. doi: 10.4153/CMB-2003-007-0.

[7] H. Davenport, *Multiplicative Number Theory*, second edition, revised by H. L. Montgomery, Graduate Texts in Mathematics **74**, Springer, 1980, Chapters 14, 16, 19–20. doi: 10.1007/978-1-4757-5927-3.

[8] P. Erdős and R. L. Graham, *On products of factorials*, Bulletin of the Institute of Mathematics, Academia Sinica **4** (1976), 337–355. Author archive.

[9] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de L'Enseignement Mathématique **28**, Geneva, 1980, p. 67.

[10] J.-H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Inventiones Mathematicae **75** (1984), 561–584. doi: 10.1007/BF01388644.

[11] Z. Kabluchko and A. Marynych, *Divisibility properties of polynomial expressions of random integers*, Journal of Number Theory **259** (2024), 357–377. doi: 10.1016/j.jnt.2024.01.017.

[12] K. S. Kedlaya, *Notes on analytic number theory*, Chapter 11, §§11.1–11.2. Online text, accessed 26 November 2026.

[13] O. Klurman, I. D. Shkredov and M. W. Xu, *On the random Chowla conjecture*, Geometric and Functional Analysis **33** (2023), 749–777. doi: 10.1007/s00039-023-00641-y.

[14] D. Krumm, *Squarefree parts of polynomial values*, Journal de Théorie des Nombres de Bordeaux **28** (2016), 699–724. doi: 10.5802/jtnb.959.

[15] F. Luca and P. G. Walsh, *On a Diophantine equation related to a conjecture of Erdős and Graham*, Glasnik Matematički, Ser. III, **42(62)** (2007), 281–289. doi: 10.3336/gm.42.2.03.

[16] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Mathematical Journal **118** (2003), 353–373. doi: 10.1215/S0012-7094-03-11826-8.

[17] B. Pouly, *Simultaneous quadratic probes: reconstruction thresholds and marked Poisson limits*, 2026. doi: 10.5281/zenodo.24443281. Public text.

[18] B. Pouly, *Small roots of split quadratic congruences and fundamental units in a quartic family*, 2026. doi: 10.5281/zenodo.24443299. Public text.

[19] I. Pylaiev, *Random Chowla and Goldbach Conjectures*, 2026. arXiv:2611.14579v1. doi: 10.48550/arXiv.2611.14579.

[20] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen der Preußischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse (1929), no. 1, 1–70.

[21] M. Skałba, *Products of disjoint blocks of consecutive integers which are powers*, Colloquium Mathematicum **98** (2003), 1–3. doi: 10.4064/cm98-1-1.

[22] M. Ulas, *On products of disjoint blocks of consecutive integers*, L'Enseignement Mathématique (2) **51** (2005), 331–334. doi: 10.5169/seals-3601.

[23] R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem*, Acta Mathematica **174** (1995), 147–240. doi: 10.1007/BF02392467.

[24] V. Y. Wang and M. W. Xu, *Paucity phenomena for polynomial products*, Bulletin of the London Mathematical Society **56** (2024), 2718–2726. doi: 10.1112/blms.13095.